

1 George Haines, Esq.
2 Nevada Bar No. 9411
3 Gerardo Avalos, Esq.
4 Nevada Bar No. 15171
FREEDOM LAW FIRM
5 8985 S. Eastern Ave., Suite 350
6 Las Vegas, NV 89123
7 Tele. 702.880.5554
8 E-fax: 702.967.6666
9 Email: info@freedomlegalteam.com

7 *Attorneys for Plaintiffs Shelby Harmer,
8 and on behalf of all others similarly situated*

10 **UNITED STATES DISTRICT COURT**

11 **DISTRICT OF NEVADA**

12 SHELBY HARMER, INDIVIDUALLY
13 AND ON BEHALF OF ALL OTHERS
14 SIMILARLY SITUATED,

16 PLAINTIFFS,

17 -VS.-

19 SAMSUNG ELECTRONICS
20 AMERICA, INC.,

21 DEFENDANT.

CASE NO.

Dept. No.:

CLASS ACTION

Complaint for Damages Based on: (1)
Negligence; (2) Invasion of Privacy; (3)
Breach of Contract; (4) Breach of
Implied Contract; And (5) Violation of
NRS 598

Jury Trial Demanded

Introduction

1. Defendant Samsung Electronics America, Inc., (hereinafter “Defendant” and/or “Samsung”) failed to safeguard the confidential personal identifying information of Plaintiff Shelby Harmer and thousands of individuals (hereinafter referred to as “Class Members” or collectively as the “Class”).
 2. This class action is brought on behalf of Samsung’s customers whose personally identifiable information (“PII” or “Private Information”) was stolen by cybercriminals in a cyber-attack that accessed sensitive information through Samsung’s U.S. systems.
 3. On or around August 4, 2022, a group of cybercriminals had access to certain files on Defendant’s computer network and servers containing personal information belonging to the Class Members.
 4. Plaintiff and Class Members were not notified of the data breach until September 2, 2022, almost one month after their information was first accessed.
 5. The cybercriminals accessed insufficiently protected information belonging to Plaintiff and the Class Members.
 6. Upon information and belief, as a result of Defendant’s failure to properly secure Plaintiff’s and the Class Members’ personal information, the cybercriminals obtained extensive personal information including names, name, contact and demographic information, date of birth, and product registration information. (“PII” or “Private Information”).
 7. As a result of Defendant’s actions and/or inaction, Plaintiff and the Class Members were harmed and forced to take remedial steps to protect themselves from future loss. Indeed, Plaintiff and all of the Class Members are currently at a very high risk of misuse of their Private Information in the coming months and years, including but not limited to unauthorized credit card charges, unauthorized access to email accounts, identity theft, and other fraudulent use of their financial accounts.
 8. Defendant’s wrongful actions and/or inaction constitute common law negligence, invasion of privacy by the public disclosure of private facts, breach of contract, and breach of implied contract.

9. Plaintiff, on behalf of themselves and the Class seeks (i) actual damages, economic damages, emotional distress damages, statutory damages and/or nominal damages, (ii) exemplary damages, (iii) injunctive relief, and (iv) fees and costs of litigation.

Jurisdiction and Venue

10. Jurisdiction of this Court arises pursuant to 28 U.S.C. §1331; 15 U.S.C. § 1681p; and, 28 U.S.C. § 1367 for supplemental state claims.

11. This Court has personal jurisdiction over Defendant through its business operations in this District, the specific nature of which occurs in this District. Defendant intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

12. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District, and because Plaintiff resides in this District.

Parties

13. Plaintiff is a natural person residing in Clark County, Nevada. In addition, Plaintiff is a “consumer” as that term is defined by 15 U.S.C. § 1692a(3) and 15 U.S.C. § 1681a(c).

14. Defendant is a computer and electronics manufacturing company, which operates nationally, including in Nevada.

Factual Allegations

15. Identity theft, which costs Americans billions of dollars a year, occurs when an individual's personal identifying information is used without his or her permission to commit fraud or other crimes. Victims of identity theft typically lose hundreds of hours dealing with the crime, and they typically lose hundreds of dollars.

16. According to the Federal Trade Commission (“FTC”):

Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit

1 reports. In rare cases, they may even be arrested for crimes they did not
2 commit.

- 3 17. The United States Government Accountability Office (“GAO”) has stated that identity
4 thieves can use identifying data to open financial accounts and incur charges and credit in
5 a person’s name. As the GAO has stated, this type of identity theft is the most damaging
6 because it may take some time for the victim to become aware of the theft and can cause
7 significant harm to the victim’s credit rating. Like the FTC, the GAO explained that victims
8 of identity theft face “substantial costs and inconvenience repairing damage to their credit
9 records,” as well the damage to their “good name.”
- 10 18. Identity theft crimes often encompass more than just immediate financial loss. Identity
11 thieves often hold onto stolen personal and financial information for several years before
12 using and/or selling the information to other identity thieves.
- 13 19. Accordingly, federal and state legislatures have passed laws to ensure companies protect
14 the security of sensitive personally identifying confidential information, such as that
15 wrongfully disclosed by Defendant.
- 16 20. The FTC has issued a publication entitled “Protecting Personal Information: A Guide for
17 Business” (“FTC Report”). The FTC Report provides guidelines for businesses on how to
18 develop a “sound data security plan” to protect against crimes of identity theft. To protect
19 the personal sensitive information in their files, the FTC Report instructs businesses to
20 follow, among other things, the following guidelines:
- 21 a. Know what personal information you have in your files and on your computers;
22 b. Keep only what you need for your business;
23 c. Protect the information that you keep;
24 d. Properly dispose of what you no longer need;
25 e. Control access to sensitive information by requiring that employees use “strong”
26 passwords; tech security experts believe the longer the password, the better; and
27 f. Implement information disposal practices reasonable and appropriate to prevent an
28 unauthorized access to personally identifying information.

- 1 21. The FTC Report also instructs companies that outsource any business functions to
- 2 proactively investigate the data security practices of the outsourced company and examine
- 3 their standards.
- 4 22. The Federal Trade Commission (“FTC”) has concluded that a company’s failure to maintain
- 5 reasonable and appropriate data security for consumers’ sensitive personal information is
- 6 an “unfair practice” in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide*
- 7 *Corp.*, 799 F.3d 236 (3d Cir. 2015).
- 8 23. Upon information and belief, Defendant has policies and procedures in place regarding the
- 9 safeguarding of confidential information it is entrusted with and Defendant failed to comply
- 10 with those policies.
- 11 24. Defendant also negligently failed to comply with industry standards or even implement
- 12 rudimentary security practices, resulting in Plaintiff’s and the Class’ confidential
- 13 information being substantially less safe than had this information been entrusted with other
- 14 similar companies.
- 15 25. In or around August 4, 2022, Plaintiff and thousands of Class Members received
- 16 notifications from Defendant it learned of suspicious activity that allowed one or more
- 17 cybercriminals to access its systems through a ransomware attack.
- 18 26. The September 2022 Notice disclosed that hackers had accessed Defendant’s systems.
- 19 27. The hackers were able to access Plaintiff’s personal information because Defendant failed
- 20 to take reasonable measures to protect the Personally Identifiable Information it collected
- 21 and stored.
- 22 28. Among other things, Defendant failed to implement data security measures designed to
- 23 prevent this attack.
- 24 29. Defendant’s notice of Data Breach was not just untimely but woefully deficient, failing to
- 25 provide basic details, including but not limited to, how unauthorized parties accessed its
- 26 networks, whether the information was encrypted or otherwise protected, how it learned of
- 27 the Data Breach, whether the breach occurred system-wide, whether servers storing
- 28 information were accessed, and how many patients were affected by the Data Breach.

- 1 30. As a result of Defendant's failure to properly secure Plaintiff's and the Class Members'
- 2 personal identifying information, Plaintiff's and the Class Members' privacy has been
- 3 invaded.
- 4 31. Moreover, all of this personal information is likely for sale to criminals on the dark web,
- 5 meaning that unauthorized parties have accessed and viewed Plaintiff's and the Class
- 6 Members' unencrypted, non-redacted information, including as name, contact and
- 7 demographic information, date of birth, and product registration information..
- 8 32. Given all of the information obtained, the criminals would also be able to create numerous
- 9 fake accounts and sell sensitive information, as part of their identity theft operation.
- 10 33. As a direct and proximate result of Defendant's wrongful disclosure, criminals now have
- 11 Plaintiff's and the Class Members' personal identifying information.
- 12 34. Additionally, the disclosure makes Plaintiff and Class Members much more likely to
- 13 respond to requests from Defendant or law enforcement agencies for more personal
- 14 information, such as bank account numbers, login information or even Social Security
- 15 numbers.
- 16 35. Because criminals know this and are capable of posing as Defendant or law enforcement
- 17 agencies, consumers like Plaintiff and their fellow Class Members are more likely to
- 18 unknowingly give away their sensitive personal information to other criminals.
- 19 36. Defendant's wrongful actions and inaction here directly and proximately caused the public
- 20 disclosure of Plaintiff's and Class Members' personal identifying information without their
- 21 knowledge, authorization and/or consent.
- 22 37. As a further direct and proximate result of Defendant's wrongful actions and/or inaction,
- 23 Plaintiff and Class Members have suffered, and will continue to suffer, damages including,
- 24 without limitation, expenses for credit monitoring and identity theft insurance, out-of-
- 25 pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-
- 26 economic harm.
- 27 38. Plaintiff and Class Members are now required to monitor their accounts and to respond to
- 28 identity theft.
- 29 39. Plaintiff and Class Members now face a very high risk of identity theft.

1 40. Names and dates of birth, combined with contact information like telephone numbers and
2 email addresses, are very valuable to hackers and identity thieves as it allows them to access
3 users' other accounts.

4 41. Thus, even if some information was not involved in the Data Breach, the unauthorized
5 parties could use Plaintiff's and Class Members' Private Information to access other
6 information, including, but not limited to email accounts, government services accounts, e-
7 commerce accounts, payment card information, and financial accounts, to engage in the
8 fraudulent activity identified by Plaintiff.

9 42. Despite disregarding its obligations to protect the sensitive information that Plaintiff and
10 Class Members entrusted it with, Defendant has not offered Plaintiff and Class Members
11 any monetary compensation or even assistance with identity protection services.

14 44. Defendant was also aware of the significant repercussions that would result from its failure
15 to do so.

Class Action Allegations

17 45. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff bring this class action on behalf of
18 themselves and the following Class of similarly situated individuals:

All persons whose sensitive personal information, including, but not limited to, name, contact and demographic information, date of birth, and product registration information that was obtained by an unauthorized individual or individuals from Defendant during the August 2022 data breach.

25 47. The putative Class is comprised of over 3,000 persons, making joinder impracticable. The
26 joinder of the Class Members is impractical and the disposition of their claims in the Class
27 action will provide substantial benefits both to the parties and to the Court. The Class can
28 be identified through Defendant's records or Defendant's agents' records.

29 48. The rights of each Class Member were violated in an identical manner as a result of
Defendant's willful, reckless and/or negligent actions and/or inaction.

- 1 49. The questions of law and fact common to all Class Members, and which predominate over
2 any questions affecting only individual Class Members, are as follows:
- 3 a. Whether Defendant negligently failed to maintain and execute reasonable procedures
4 designed to prevent unauthorized access to Plaintiff's and Class Members' personal
5 identifying information;
- 6 b. Whether Defendant was negligent in storing and failing to adequately safeguard Plaintiff's
7 and Class Members' personal identifying information;
- 8 c. Whether Defendant owed a duty to Plaintiff and Class Members to exercise reasonable
9 care in protecting and securing their personal identifying information;
- 10 d. Whether Defendant breached its duties to exercise reasonable care in failing to protect and
11 secure Plaintiff's and Class Members' personal identifying information;
- 12 e. Whether by disclosing Plaintiff's and Class Members' personal identifying information
13 without authorization, Defendant invaded Plaintiff's and Class Members' privacy;
- 14 f. Whether Defendant created an implied contract with Plaintiff and Class Members to keep
15 their personal identifying information confidential; and
- 16 g. Whether Plaintiff and Class Members sustained damages as a result of Defendant's failure
17 to secure and protect their personal identifying information.
- 18 50. Plaintiff and their counsel will fairly and adequately represent the interests of Class
19 Members.
- 20 51. Plaintiff has no interests antagonistic to, or in conflict with, Class Members' interests.
- 21 52. Plaintiff's attorneys are experienced in the prosecution of consumer class action, complex
22 litigation and privacy breach cases.
- 23 53. Plaintiff's claims are typical of Class Members' claims in that Plaintiff's claims and Class
24 Members' claims all arise from Defendant's wrongful disclosure of their personal
25 identifying information and from Defendant's failure to properly secure and protect the
26 same.
- 27 54. A class action is superior to all other available methods for fairly and efficiently
28 adjudicating Plaintiff's and Class Members' claims. Plaintiff and Class Members have been
29 irreparably harmed as a result of Defendant's wrongful actions and/or inaction.

- 1 55. Litigating this case as a class action will reduce the possibility of repetitious litigation
2 relating to Defendant's failure to secure and protect Plaintiff's and Class Members' personal
3 identifying information.
- 4 56. Class certification, therefore, is appropriate pursuant to Rule 23 because the above common
5 questions of law or fact predominate over any questions affecting individual Class
6 Members, and a class action is superior to other available methods for the fair and efficient
7 adjudication of this controversy.
- 8 57. Class certification also is appropriate pursuant Federal Rule of Civil Procedure 23 because
9 Defendant has acted or refused to act on grounds generally applicable to the Class, so that
10 final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a
11 whole.
- 12 58. The expense and burden of litigation would substantially impair the ability of Class
13 Members to pursue individual lawsuits in order to vindicate their rights.
- 14 59. Absent a class action, Defendant will retain the benefits of their wrongdoing despite its
15 serious violations of the law.

16 **First Cause of Action**
17 **Negligence**

- 18 60. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set
forth herein.
- 19 61. Upon Defendant's accepting and storing the Private Information of Plaintiff and the Class
20 in its computer systems and on its networks, Defendant undertook and owed a duty to
21 Plaintiff and the Class to exercise reasonable care to secure and safeguard that information
22 and to use commercially reasonable methods to do so. Defendant knew that the Private
23 Information was private and confidential and should be protected as private and
24 confidential.
- 25 62. Defendant owed a duty of care not to subject Plaintiff's and the Class's Private Information
26 to an unreasonable risk of exposure and theft because Plaintiff and the Class were
27 foreseeable and probable victims of any inadequate security practices.
- 28 63. It was reasonably foreseeable that Defendant's failure to exercise reasonable care in
29 safeguarding and protecting Plaintiff's and Class Members' personal identifying

information would result in an unauthorized third party gaining access to such information for no lawful purpose, and that such third parties would use Plaintiff's and Class Members' personal identifying information for malevolent and unlawful purposes, including the commission of direct theft and identity theft.

64. Defendant knew, or should have known, of the risks inherent in collection and storing Private Information and the importance of adequate security.
 65. Defendant knew or should have known about numerous well-publicized data breaches within the medical industry.
 66. Plaintiff and the Class Members were (and continue to be) damaged as a direct and proximate result of Defendant's failure to secure and protect their personal identifying information as a result of, *inter alia*, direct theft, identity theft, expenses for credit monitoring and identity theft herein, insurance incurred in mitigation, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm, for which they suffered loss and are entitled to compensation.
 67. Defendant's wrongful actions and/or inaction (as described above) constituted (and continue to constitute) negligence at common law.

Second Cause of Action Invasion of Privacy by Public Disclosure of Private Facts and Intrusion Upon Seclusion

68. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.
 69. Plaintiff's and Class Members' personal identifying information is and always has been private information.
 70. Dissemination of Plaintiff's and Class Members' private information is not of a legitimate public concern; publication to third parties of their personal identifying information would be, is and will continue to be, offensive to Plaintiff, Class Members, and other reasonable people.
 71. Plaintiff and the Class Members were (and continue to be) damaged as a direct and proximate result of Defendant's invasion of their privacy by publicly disclosing their private facts including, *inter alia*, direct theft, identity theft, expenses for credit monitoring and

1 identity theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy,
2 and other economic and non-economic harm, for which they are entitled to compensation.

3 72. Defendant's wrongful actions and/or inaction (as described above) constituted (and
4 continue to constitute) an invasion of Plaintiff's and Class Members' privacy by publicly
5 disclosing their private facts (*i.e.*, their personal identifying information).

6
7 **Third Cause of Action**
8 **Breach of Contract**

9 73. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set
forth herein.

10 74. Plaintiff and other Class Members entered into valid and enforceable express contracts with
11 Defendant under which Plaintiff and other Class Members agreed to provide their Private
12 Information to Defendant, and Defendant agreed to provide medical services and, impliedly,
13 if not explicitly, agreed to protect Plaintiff's and Class Members' Private Information.

14 75. To the extent Defendant's obligation to protect Plaintiff's and other Class Members' Private
15 Information was not explicit in those express contracts, the express contracts included
16 implied terms requiring Defendant to implement data security adequate to safeguard and
17 protect the confidentiality of Plaintiff's and other Class Members' Private Information,
18 including in accordance with federal, state and local laws; and industry standards.

19 76. Neither Plaintiff nor any Class member would have entered into these contracts with
20 Defendant without the understanding that Plaintiff's and other Class Members' Private
21 Information would be safeguarded and protected; stated otherwise, data security was an
22 essential implied term of the parties' express contracts.

23 77. A meeting of the minds occurred, as Plaintiff and Class Members agreed, among other
24 things, to provide their Private Information in exchange for Defendant's agreement to
25 protect the confidentiality of that Private Information.

26 78. The protection of Plaintiff's and Class Members' Private Information were material aspects
27 of Plaintiff and Class Members' contracts with Defendant.

79. Defendant's promises and representations described above relating industry practices, and Defendant's purported concern about its clients' privacy rights became terms of the contracts between Defendant and its clients, including Plaintiff and other Class Members.
 80. Defendant breached these promises by failing to comply with reasonable industry practices.
 81. Plaintiff and Class Members read, reviewed, and/or relied on statements made by or provided by Defendant and/or otherwise understood that Defendant would protect its patients' Private Information if that information were provided to Defendant.
 82. Plaintiff and Class Members fully performed their obligations under the implied contract with Defendant; however, Defendant did not.
 83. As a result of Defendant's breach of these terms, Plaintiff and Class Members have suffered a variety of damages including but not limited to: the lost value of their privacy; not getting the benefit of their bargain with Defendant; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, the requirement to place "freezes" and "alerts" with credit reporting agencies, to contact financial institutions, to close or modify financial accounts, to closely review and monitor credit reports and various accounts for unauthorized activity, and to file police reports.
 84. Additionally, Plaintiff and Class Members have been put at an increased risk of future identity theft, fraud, and/or misuse of their Private Information, which may take years to manifest, discover, and detect.
 85. Plaintiff and Class Members are therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and fees and costs of litigation.

Fourth Cause of Action Breach of Implied Contract

86. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.
 87. “Where the terms of a contract are literally complied with but one party to the contract deliberately contravenes the intention and spirit of the contract, that party can incur liability

1 for breach of the implied covenant of good faith and fair dealing.” *Hilton Hotels Corp. v.*
2 *Butch Lewis Prods., Inc.*, 107 Nev. 226, 232 (1991).

3 88. Among other things, Plaintiff and Class Members were required to disclose their personal
4 identifying information to Defendant in order to obtain the Defendant’s goods and services,
5 as well as implied contracts for the Defendant to implement data security adequate to
6 safeguard and protect the privacy of Plaintiff’s and Class Members’ Private Information.

7 89. When Plaintiff and Class Members provided their Private Information to Defendant in
8 exchange for Defendant’s services, they entered into implied contracts with Defendant
9 pursuant to which Defendant agreed to reasonably protect such information.

10 90. In entering into such implied contracts, Plaintiff and Class Members reasonably believed
11 and expected that Defendant’s data security practices complied with relevant laws and
12 regulations and were consistent with industry standards.

13 91. Class Members who paid money to Defendant reasonably believed and expected that
14 Defendant would use part of those funds to obtain adequate data security.

15 92. Defendant failed to do so.

16 93. Under implied contracts, Defendant and/or its affiliated providers promised and were
17 obligated to: (a) provide goods and services to Plaintiff and Class Members; and (b) protect
18 Plaintiff’s and Class Members’ Private Information provided to obtain the benefits of such
19 services.

20 94. In exchange, Plaintiff and Members of the Class agreed to pay money for these services,
21 and to turn over their Private Information.

22 95. Plaintiff and Class Members performed their obligations under the contract when they paid
23 for Defendant’s goods and services and provided their Private Information.

24 96. Defendant materially breached its contractual obligation to protect the private information
25 Defendant gathered when the information was accessed and exfiltrated during the Data
26 Breach.

27 97. Defendant materially breached the terms of the implied contracts.

28 98. Defendant did not maintain the privacy of Plaintiff’s and Class Members’ Private
29 Information as evidenced by its notifications of the Data Breach to Plaintiff and Class
Members.

99. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiff's and Class Members' private information as set forth above.
 100. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.
 101. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Class Members did not receive full benefit of the bargain they entered into, and instead received goods and services that were of a diminished value to that described in the contracts.
 102. Plaintiff and Class Members, therefore, were damaged in an amount at least equal to the difference in the value between the goods and services they paid for as compared to what they received.
 103. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, Class Members, nor any reasonable person would have purchased goods and services from Defendant and/or its affiliated providers.
 104. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, out of pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant

Fifth Cause of Action
Violation of Nevada Deceptive Trade Practices Act
Nev. Rev. Stat. §598. et Seq.

105. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.
 106. This cause of action is brought pursuant to the Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. §§598 *et seq.*, (the “Nevada Act”).

107. Defendant sells electronic and computer goods and services to the general public.
Defendant's activities are governed by the State Consumer Protection Acts.
108. On information and belief, affected individuals include persons over the age of 60 and
persons with disabilities.
109. In all requisite matters alleged herein, Defendant acted in the course of their business or
occupation within the meaning of NRS §§598.0903 to 598.0999.
110. In all requisite matters alleged herein, Defendant acted willfully in violation of NRS §598.
111. Defendant violated NRS §598 by engaging in the unfair and deceptive practices as
described herein which offend public policies and are immoral, unethical, unscrupulous and
substantially injurious to consumers.
112. Reasonable customers would be misled by Defendant's misrepresentations and omissions
concerning the security of their personally identifying information.
113. Defendant's unfair and deceptive practices are thus likely to, and have, misled the Class
Members acting reasonably in the circumstances, in violation of NRS §598.
114. Defendant specifically engaged in the following activity, all of which violate NRS §598:
 - a. Defendant failed to maintain and execute reasonable procedures designed to prevent
unauthorized access to Plaintiff's and Class Members' personal identifying
information;
 - b. Defendant acted unlawfully in improperly storing and failing to adequately
safeguard Plaintiff's and Class Members' personal identifying information;
 - c. Defendant failed to exercise reasonable care in protecting and securing their
personal identifying information;
 - d. Defendant failed to properly and timely notify Plaintiff and the Class about the
severity of the breach, including failure to provide an adequate description of the
breach and the risks associated with the breach.
115. In all requisite matters alleged herein, Defendant acted knowingly within the meaning of
NRS §598.
116. In all requisite matters alleged herein, Defendant acted willfully in violation of NRS §598.
117. Plaintiff and Class Members have been aggrieved by Defendant's unfair and deceptive
practices including because they have lost control of their personally identifying

1 information, and they have to expend out of pocket money and efforts to mitigate the harm
2 caused by Defendant.

3 118. Pursuant to NRS §598, Plaintiff and the Class Members seek a declaratory judgment and
4 court order enjoining the above-described wrongful acts and practices of Defendant.
5 Additionally, Plaintiff and the Class Members make claims for damages, and fees and costs
6 of litigation.

7 **Prayer for Relief**

8 119. Wherefore, Plaintiff, individually and on behalf of the other members of the Class proposed
9 in this complaint, respectfully request that the Court enter judgement in favor of Plaintiffs
10 and the Class against Defendant, as follows:

- 11 • Certifying this action as a class action, with a class as defined above;
- 12 • For equitable relief enjoining Defendant from engaging in the wrongful
13 acts and omissions complained of herein pertaining to the misuse and/or
14 disclosure of Plaintiff's and Class Members' Private Information, and
15 from failing to issue prompt, complete and accurate disclosures to
16 Plaintiff and Class Members;
- 17 • Awarding compensatory damages to redress the harm caused to Plaintiff
18 and Class Members in the form of, *inter alia*, direct theft, identity theft,
19 expenses for credit monitoring and identity theft insurance, out-of-
20 pocket expenses, anxiety, emotional distress, loss of privacy, and other
21 economic and non-economic harm. Plaintiff and Class Members also are
22 entitled to recover statutory damages and/or nominal damages.
23 Plaintiff's and Class Members' damages were foreseeable by Defendant
24 and exceed the minimum jurisdictional limits of this Court.
- 25 • Ordering injunctive relief including, without limitation, (i) adequate
26 credit monitoring, (ii) adequate identity theft insurance, (iii) instituting
27 security protocols in compliance with the appropriate standards and (iv)
28 requiring Defendant to submit to periodic compliance audits by a third
29 party regarding the security of personal identifying information in its
possession, custody and control.

- Awarding Plaintiff and the Class Members interest, costs and attorneys' fees; and
 - Awarding Plaintiff and the Class such other and further relief as this Court deems just and proper.

Trial by Jury

120. Pursuant to the seventh amendment to the Constitution of the United States of America and
the Constitution of the State of Nevada, Plaintiff is entitled to, and demands, a trial by jury.

DATED this 6th day of September 2022.

FREEDOM LAW FIRM

/s/ George Haines

George Haines, Esq.
Gerardo Avalos, Esq.
8985 South Eastern Ave., Suite 350
Las Vegas, NV 89123
*Attorneys for Plaintiff and on behalf
of all others similarly situated*